LATHAM & WATKINS LLP
Melanie M. Blunschi (Bar No. 234264)
melanie.blunschi@lw.com
Kristin Sheffield-Whitehead (Bar No. 304635)
kristin.whitehead@lw.com
505 Montgomery St., Suite 2000
San Francisco, CA 94111
Telephone: +1.415.391.0600

Andrew B. Clubok (*pro hac vice*)
andrew.clubok@lw.com
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Telephone: +1.202.637.2200

Michele D. Johnson (Bar No. 198298)
michele.johnson@lw.com
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626
Telephone: +1.714.540.1235

ELIZABETH K. MCCLOSKEY (SBN 268184)
EMcCloskey@gibsondunn.com
ABIGAIL A. BARRERA (SBN 301746)
ABarrera@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Meta Platforms, Inc.
(formerly known as Facebook, Inc.)

[Additional Counsel Listed Below]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ERICA FRASCO et al.,

Plaintiffs,

v.

FLO HEALTH, INC., GOOGLE LLC, FACEBOOK, INC., and FLURRY, INC.,

Defendants.

CASE NO. 3:21-CV-00757-JD (consolidated)

DEFENDANT META PLATFORMS, INC.'S NOTICE OF MOTION AND MOTION FOR SUMMARY JUDGMENT

Judge:	Hon. James Donato
Court:	Courtroom 11 – 19th Floor
Date:	April 24, 2025
Time:	10:00 a.m.

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT, on April 24, 2025, at 10:00 a.m., the undersigned will appear before the Honorable James Donato of the United States District Court for the Northern District of California at the San Francisco Courthouse, Courtroom 11, 19th Floor, 450 Golden Gate Avenue, San Francisco, CA 94102, and shall then and there present this motion for summary judgment on behalf of Defendant Meta Platforms, Inc.

Meta brings this motion under Rule 56 of the Federal Rules of Civil Procedure. Meta will, and hereby does, move for an order granting summary judgment in Meta's favor because there is no genuine dispute of material fact as to any of the claims against Meta, and Meta is entitled to judgment as a matter of law. The motion is based on this notice of motion, the following memorandum of points and authorities and the exhibits attached thereto, the pleadings and other papers filed in this action, any oral argument, and any other evidence that the Court may consider in deciding this motion.

ISSUES PRESENTED

Whether Meta is entitled to summary judgment under Federal Rule of Civil Procedure 56 because the undisputed facts establish that plaintiffs cannot prove essential elements of their California Invasion of Privacy Act, federal Wiretap Act, Comprehensive Computer Data Access and Fraud Act, Unfair Competition Law, and "aiding and abetting" claims.

Dated: February 6, 2025

/s/ Elizabeth K. McCloskey

GIBSON, DUNN & CRUTCHER LLP
Elizabeth K. McCloskey (SBN 268184)
EMcCloskey@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200
Facsimile: 415.393.8306

Counsel for Defendant Meta Platforms, Inc.
(formerly known as Facebook, Inc.)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES
(*Cont'd.*)

Page(s)

TABLE OF AUTHORITIES
(*Cont'd.*)

TABLE OF AUTHORITIES
(*Cont'd.*)

Page(s)

Statutes

TABLE OF AUTHORITIES
(*Cont'd.*)

Other Authorities

Rules

INTRODUCTION

Plaintiffs, users of Flo's period-tracking app, sued Meta and others on the theory that they intentionally "intercepted," "hacked," and "eavesdropped" on plaintiffs' health-related communications with Flo, violating the Wiretap Act, CIPA, CDAFA, UCL, and aiding and abetting Flo's violation of their privacy and the UCL. But four years of litigation have shown that plaintiffs' theory is impossible to square with the undisputed facts, including: (1) Meta did not "intercept," "hack," or "eavesdrop" on anything—Meta simply received data that Flo created and chose to send; (2) the challenged communications were between Flo and Meta—plaintiffs were not involved in those communications, meaning they cannot bring wiretapping, eavesdropping, or hacking claims, and meaning Meta, as a party to those communications, could not "intercept," "hack," or "eavesdrop" on them; and (3) Meta did not intend for Flo to send it health information—to the contrary, Meta expressly prohibited Flo from doing so. For these reasons and others, plaintiffs cannot prove essential elements of their claims, and the Court should grant summary judgment to Meta.

First, plaintiffs cannot prove their Wiretap Act and CIPA claims for at least four reasons:

No "interception" of plaintiffs' communications with Flo. Plaintiffs' theory centers on a software-development kit ("SDK") created by Meta. Meta's SDK helps app developers like Flo monitor and improve the performance of their apps. Flo incorporated Meta's SDK into its app code and, as is customary, named the "Custom Events" that the Flo app would send to Meta if users took certain actions in the app. The undisputed facts—developed over two years of discovery—show that Meta did not "intercept" plaintiffs' communications with Flo. To "intercept" something is to reach in and grab it while it is being sent from a sender to a recipient. But here, the Flo app created and sent the Custom Events directly to Meta. Plaintiffs were never a party to those communications. And under binding precedent, Meta cannot be held liable for receiving communications that Flo sent to Meta, just as retrieving mail from one's own mailbox is not a crime.

No "interception" while "in transit." The Wiretap Act and CIPA § 631(a) prohibit "interception" when information is "in transit," and information that is *stored* before being sent—even for milliseconds—is not "in transit." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). It is indisputable that the information Flo sent to Meta was stored before it was transmitted.

No intent to "intercept" or "eavesdrop." An independent problem with plaintiffs' interception theory is that there is no evidence that Meta "intended" to "intercept" or "eavesdrop" on any health-related communications between plaintiffs and Flo. In fact, Meta expressly prohibited Flo and others using its SDK from sending "health" or other "sensitive" information, as well as any information without "all necessary rights and permissions," and there is no evidence suggesting Meta nevertheless actually sought that information. Courts have declined to hold defendants liable for receiving unwanted health information, *e.g.*, *Doe I v. Google LLC*, 2024 WL 3490744 (N.D. Cal. July 22, 2024), and this Court should do the same.

Barred by consent. Lack of consent is a required element of plaintiffs' CIPA claims, and consent is a complete defense to their Wiretap Act claim. Here, seven of the eight plaintiffs consented to the data sharing they now challenge, because they used Facebook, one of Meta's services, and agreed to its data-sharing policies. Those policies have consistently made clear that Meta may receive data reflecting users' activity on apps that use Meta's SDK, stating, for example, that Meta "collect[s] different kinds of information . . . about [users]," including "information when [they] visit or use third-party . . . apps that use [Meta's] Services" and information "about the . . . apps [they] visit." App. 39. The Court's ruling on the issue of consent in connection with Google's motion for summary judgment does not foreclose this argument with respect to Meta, because the Court concluded "Google hangs its hat for the defense of consent solely on plaintiffs' acceptance of Flo's privacy policies." Dkt. 485 at 3–4. The Court did not consider Meta's disclosures, which were consistent and explicit. Courts regularly dismiss or grant summary judgment on claims just like those asserted here when the plaintiffs agreed to the very types of disclosures they challenged—including in cases against Meta. *E.g.*, *Smith v. Facebook, Inc.*, 745 F. App'x 8 (9th Cir. 2018). Moreover, there is no Wiretap Act violation when any party to the communication consents to sharing it, so Flo's consent to the data sharing suffices for that claim.

Second, plaintiffs cannot prove essential elements of their CDAFA claim. There is no evidence Meta "actively participated" in the "hacking" required by the statute, much less evidence Meta *knowingly* "hacked" any device or data. At most, Meta passively received information from Flo. And because plaintiffs consented to Meta's data-sharing policies, they cannot prove CDAFA's "without permission" element. But even if the Court assumed Meta actively and knowingly "hacked" plaintiffs' devices without permission, plaintiffs still could not prevail because they cannot show any resulting damage or loss. Nearly every court to decide the issue has held that an invasion of privacy alone does not qualify as "damage or loss" under the CDAFA. *E.g.*, *Heiting v. Taro Pharm. USA, Inc.*, 709 F. Supp. 3d 1007, 1020 (C.D. Cal. 2023). Although this Court was one of the few to depart from that consensus in deciding Google's summary-judgment motion (Dkt. 485 at 4–5), it should revisit that analysis in light of the many contrary cases not cited in previous briefing on this issue.

Third, as the Court determined in resolving Google's motion for summary judgment (Dkt. 485 at 5–6), plaintiffs cannot prove their "aiding and abetting" intrusion-upon-seclusion claim because they cannot offer evidence that Meta knew about Flo's allegedly deceptive disclosure practices, much less that Meta substantially assisted or encouraged Flo to make allegedly false representations. And, in any event, plaintiffs' consent to the data sharing they challenge bars this claim.

Fourth, plaintiffs cannot prove their UCL and corresponding "aiding and abetting" claims because there is no evidence plaintiffs have "lost money or property," Cal. Bus. & Prof. Code § 17204, there is no evidence showing Meta had the requisite mens rea for the "aiding and abetting" claim, and both claims are barred by consent.

Although this case is notionally about only Flo's use of SDKs created by Meta and others, it is really about whether plaintiffs here (and in a rash of recent cases) can radically expand what it means to "intercept," "eavesdrop," or "hack," well beyond those terms' meanings and the relevant statutes' purposes. Such an expansion would negatively impact thousands of app and web developers, who use tools like Meta's SDK—lawfully and without violating their users' privacy—to improve the functionality of their apps and websites and to add difficult-to-develop functions—both consumer-facing features, like chat functionality, and technical back-end features, like authentication, storage, and analytics. With that context in mind, and because plaintiffs cannot establish the essential elements of their claims, the Court should grant Meta's motion for summary judgment.

FACTUAL BACKGROUND

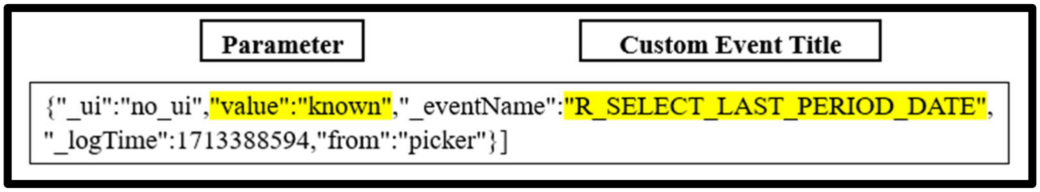
Flo's use of Meta's SDK. Plaintiffs filed this lawsuit in June 2021, alleging Flo improperly shared their health information with Meta, Google, and Flurry using those companies' SDKs. *See*

Dkt. 64. SDKs are bits of code that app developers can use for a variety of purposes, and numerous developers tailor SDKs to the needs of their specific apps. App. 497–99. Tools like the Meta SDK are a ubiquitous feature of modern life. Countless developers use these tools, which provide them with additional features—such as authentication, storage, analytics, and chat features—that they would otherwise have to spend their limited resources building from scratch for their apps and websites. *See id.* Website developers, for instance, regularly embed chat features on their webpages to communicate with their users and rely on third-party support to track and analyze customer metrics, which allow developers to improve their products and support their users. *See, e.g.*, *Licea v. Cinmar, LLC*, 659 F. Supp. 3d 1096, 1101 (C.D. Cal. 2023). Use of these tools is so widespread that Android apps each use an average of 18 different SDKs. *See* App. 499–500.

The SDK at issue here allows app developers to send data about certain actions users take in their apps to Meta, which then returns aggregated information about how users interact with the apps. App. 152–53, 502–05. Meta makes the SDK available to the public; developers decide which actions they want to track. *Id.* Developers can take Meta's generic code, use it as "they please," and change the "code as much or as little as they want." App. 270.

Like many other app developers, Flo decided to integrate Meta's SDK into its app and, as is customary, tailored the SDK code to fit its own needs, to better understand how users interacted with the app, and to improve the app's functionality. App. 163, 490, 497–99, 502–03, 506–07, 656–57; App. 713–14 (describing how SDKs become part of the app's overall code). Plaintiffs' claims against Meta are focused on eleven "Custom Events" that allegedly "conveyed reproductive health information." Dkt. 477 at 3. Custom Events are strings of code created by app developers like Flo. App. 506–07. Custom Events include a title chosen by the app developer and optional parameters (reflecting binary values, integers, or text values) that convey information about actions users take within the app. App. 282, 429–31, 463, 505–08. That is what happened here: Flo decided which user actions to track and named the corresponding Custom Events, including the eleven at issue here. App. 506–07, 571; *see* App. 125–33. Meta did not review or approve the Custom Events Flo created, and, outside of this litigation, Flo did not send Meta any kind of key or other documents that would have allowed Meta to understand the meaning of their Custom Events. App. at 268–69, 658–61.[1]

For example, plaintiffs challenge the Custom Event "R_SELECT_LAST_PERIOD_DATE," which Flo created and named. Discovery revealed this Custom Event corresponds to *whether* a user selected the date of her last period during the Flo app's one-time onboarding process (i.e., whether the information is "known" or "unknown"). App. 125. Even plaintiffs' technical expert acknowledges the Custom Event data did *not* reveal the date of users' last period, and instead revealed, at most, the Custom Event title and a parameter indicating whether users selected a date:



Parameter **Custom Event Title**

```
{"_ui":"no_ui","value":"known","_eventName":"R_SELECT_LAST_PERIOD_DATE",
"_logTime":1713388594,"from":"picker"}]
```

App. 604. In any event, Meta did not know what the Custom Event meant when it received this information and thus had no way of understanding what this Custom Event was meant to capture. App. 163–64, 571, 656–57, 658–61.

Flo's Custom Events were not contemporaneously transmitted to Meta or even transmitted as soon as they were created. App. 507–10. A Custom Event was generated only after a user performed an action that triggered a specific Custom Event. App. 507–08. And once generated, Custom Events were first cached on users' devices for varying amounts of time—from "milliseconds" to "weeks" or even longer—until certain developer-specified conditions were met. App. 507–10, 847–48. Like everything else about the SDK, developers could "modify these . . . conditions to suit their needs," including by lengthening the time that Custom Events were cached on devices before they were transmitted to Meta. App. 508–09.

Meta's Business Tools Terms. As a condition of using Meta's SDK, Flo—like all app developers—agreed to Meta's Business Tools Terms. App. 502–03, 666–68. Throughout the class

[1] There are no records showing which Custom Events Meta received for a specific device or person. Nor are there records showing which Custom Event parameters Meta may have received. Because plaintiffs did not sue until 2021 but base their claims on data sent from 2016 to 2019, any device-level information received by Meta was deleted in the ordinary course of business, consistent with Meta's retention policies. App. 187. Meta has only aggregate records showing the Custom Event titles it received during the relevant period.

period, those terms prohibited Flo and other developers from sending Meta "health" information or any other types of "sensitive personal data." App. 9; *see, e.g.*, App. 13, 17, 20, 25, 668. Those terms also required Flo and other developers to have "all necessary rights and permissions" before sending any data to Meta using tools like the SDK. App. 274 ("Flo Health agreed to the business tool terms"); *see, e.g.*, App. 9. And the terms required Flo and other developers to "provide[] robust and sufficiently prominent notice to users regarding the Customer Data collection, sharing and usage." App. 21–22. These conditions reflect the reality that Meta is not involved in developers' relationships with their users, and Meta does not have any way to interpret the data those developers collect; as a result, developers are best positioned to ensure they are not sending Meta prohibited information and disclose their use of Meta's SDK to their users.

Meta's Data Policy. Even though Meta required developers to disclose and obtain consent to their use of Meta's SDK, Meta also informed its users that it would collect data about their use of apps that integrated its SDK. During the relevant period, all users of Facebook, one of Meta's services, had to agree to certain terms and policies, including Meta's Data Policy. App 879–81. Throughout the class period, that policy informed Meta's users that Meta "collect[s] different kinds of information from or about [them]," including "[i]nformation from websites and apps that use [Meta's] Services" like the SDK. App. 39; *see also, e.g.*, App. 33, 47, 57–58. The policy explained that Meta "collect[s] information when you visit or use third-party websites and apps that use our services (like when they . . . use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or [Meta]." App. 39; *see also, e.g.*, App. 33, 47, 57–58.

2019 *Wall Street Journal* article. Meta first learned of allegations that Flo was sending it health information via its SDK when *The Wall Street Journal* published an article about the data-sharing practices of Flo and other app developers in February 2019. App. 272–73. Upon learning of these allegations, Meta built out its systems to detect and filter out "potentially health-related terms." App. 272–73, 275.

Discovery in this case. Extensive discovery began following the Court's order granting in part and denying in part defendants' motions to dismiss in June 2022. *See* Dkt. 158. As part of that discovery, Meta produced over 400,000 pages of documents. App 2. Plaintiffs also raised many discovery disputes before the Court, including seeking additional discovery into the source code for the Flo app and any Custom Event data in Flo's possession. *See* Dkt. 300, 353. Plaintiffs also retained an expert who purports to have done a "technical analysis" of several versions of the Flo app. App. 542–43.

LEGAL STANDARD

Summary judgment is warranted when "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Material facts are those that may affect the outcome of the case. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). The movant has the "initial burden to show that the nonmoving party . . . does not have enough evidence of an essential element" of a claim. *G & G Closed Circuit Events, LLC v. Liu*, 45 F.4th 1113, 1115 (9th Cir. 2022); *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 322–23 (1986). The burden then shifts to the nonmoving party to "go beyond the pleadings and by [his] own affidavits, or by the 'depositions, answers to interrogatories, and admissions on file,' designate 'specific facts showing that there is a genuine issue for trial.'" *Celotex*, 477 U.S. at 324. "The non-moving party must show more than the mere existence of a scintilla of evidence" or a "metaphysical doubt" regarding its claims, *In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 387 (9th Cir. 2010), and must instead introduce "significant probative evidence tending to support the complaint," *Rivera v. Nat'l R.R. Passenger Corp.*, 331 F.3d 1074, 1078 (9th Cir. 2003) (quoting *Anderson*, 477 U.S. at 249).

ARGUMENT

The Court should grant summary judgment to Meta because plaintiffs cannot prove essential elements of each of their claims, entitling Meta to judgment as a matter of law.

I. Plaintiffs Cannot Prove Essential Elements Of Their Wiretap Act And CIPA Claims.

Meta is entitled to summary judgment on plaintiffs' CIPA and Wiretap Act claims for four independent reasons. First, to prevail on their CIPA and Wiretap Act claims, plaintiffs must show that Meta "intercepted" or "eavesdropped" on *plaintiffs' communications* with Flo. But undisputed evidence shows that Meta did not "intercept" or "eavesdrop" on plaintiffs' communications with Flo—instead, code programmed by Flo app developers created the challenged Custom Events based on Flo app users' actions in the app, and those Custom Events were then sent by the app directly to Meta. Under even the most tortured reading of these statutes, that conduct does not amount to "intercepting" or "eavesdropping" on plaintiffs' communications with Flo. Second, the Wiretap Act and CIPA § 631(a) claims also fail because plaintiffs must prove that Meta "intercepted" or "eavesdropped" on their communications "in transit." But undisputed evidence shows Meta did not receive the challenged Custom Events while they were "in transit," because they were stored first and then sent to Meta when certain conditions were met. Third, plaintiffs must also show that Meta *intended* to "intercept" or "eavesdrop" on plaintiffs' communications, but there is no evidence that Meta had that intent. Fourth, plaintiffs' CIPA and Wiretap Act claims are barred by consent.

A. Undisputed Evidence Proves That Meta Did Not "Intercept" Or "Eavesdrop" On Plaintiffs' Communications With Flo.

The Court should reject plaintiffs' attempts to stretch the Wiretap Act and CIPA far beyond their express language and intended purpose. These claims require proof that Meta either "intercepted" or "eavesdropped" on a "communication." *See* 18 U.S.C. § 2511(1) ("intercepts . . . [or] endeavors to intercept . . . any . . . communication"); Cal. Penal Code § 631(a) ("reads, or attempts to read, or to learn the contents or meaning of any . . . communication"); Cal. Penal Code § 632(a) ("eavesdrop upon . . . [a] confidential communication"). The Wiretap Act was meant to provide protection for communications made with then-new technology (such as the telephone) that is similar to the protection afforded "against [the] unauthorized opening" of someone else's mail. S. Rep. No. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559. This is consistent with the "ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'" *Konop*, 302 F.3d at 878. Similarly, CIPA is intended to prohibit behavior akin to "an eavesdropper pressing up against a door to listen to a conversation." *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1082 (C.D. Cal. 2023) (cleaned up); *see also* Cal. Penal Code § 630. Thus, when considering the purpose of CIPA, the California Supreme Court explained: "While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor." *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021).

Here, plaintiffs' theory is that Meta "intercepted" and "eavesdropped" on plaintiffs' communications with Flo. But after two years of extensive discovery, *see supra* at p. 7, plaintiffs have not uncovered any evidence to support their theory. Instead, the undisputed evidence shows that the communications at issue—the Custom Events named by Flo and sent by the Flo app to Meta—were between the Flo app and Meta. Plaintiffs were not parties to those communications. Specifically, the undisputed evidence shows that Flo created and named the challenged Custom Events. *See supra* at pp. 4–5. Although those Custom Events were triggered by plaintiffs' interactions with the Flo app, they were created *after* plaintiffs interacted with the Flo app and included information that was *different* from their communications with Flo. *See id.* at pp. 5–6. For example, according to plaintiffs' expert, when users communicated the date of their last period or the average length of their period to Flo during the onboarding process, the Flo app would generate Custom Event titles ("R_SELECT_LAST_PERIOD_DATE" or "R_SELECT_PERIOD_LENGTH") and parameters reflecting whether the date or the length was "known" (rather than "unknown") and send those Custom Events to Meta. App. 584–85, 604. In other words, the Custom Events that the Flo app sent to Meta were a new and different communication from plaintiffs' communications with Flo. *See id.*; *supra* at pp. 4–6. Plaintiffs were not involved in and did not receive Flo's communications with Meta. *See supra* at pp. 5–6.

This series of events cannot constitute "intercepting" or "eavesdropping" for two reasons: (1) because plaintiffs' own communications were not "intercepted," they cannot assert wiretapping or eavesdropping claims; and (2) a party to a communication cannot be held liable for "wiretapping" or "eavesdropping" on its own communication. To hold otherwise would be akin to punishing Meta for opening mail that Flo created, addressed to Meta, and sent directly to Meta's own mailbox.

First, only a party to a communication that was purportedly "intercepted" or "eavesdropped" upon can bring a wiretapping or eavesdropping claim. *See* 18 U.S.C. § 2520(a) (providing private right of action for "any person whose . . . communication is intercepted"); Cal. Penal Code § 637.2(a) (providing private right of action for "[a]ny person who has been injured by a violation of [the statute]"); *Noel v. Hall*, 2006 WL 2129799, at *2 (D. Or. July 28, 2006) (holding, as to federal Wiretap Act claim, "plaintiff lacks standing to object to the copying of any conversation to which he was not a party"), *aff'd*, 568 F.3d 743, 748 (9th Cir. 2009); *Smith*, 11 Cal. 5th at 200. Because plaintiffs were not parties to the Flo app's transmission of Custom Events to Meta, and because that transmission was entirely separate from any of plaintiffs' communications with Flo, Meta did not "intercept" or "eavesdrop" on plaintiffs' communications. Plaintiffs thus have no basis to prevail on their Wiretap Act and CIPA claims. *See Noel*, 2006 WL 2129799, at *2 (granting summary judgment for defendant on Wiretap Act claim for communications to which plaintiff was not a party).

Second, plaintiffs cannot prevail on their wiretapping and eavesdropping claims for another reason: the undisputed evidence shows that *Meta* was a party to the relevant communications, and a party cannot be held liable for "wiretapping" or "eavesdropping" on its own communications. Both the Wiretap Act and CIPA 631(a) have "an exception to liability for a person who is a party to the communication." *Doe I*, 2024 WL 3490744, at *5; *see also Cody v. Boscov's, Inc.*, 658 F. Supp. 3d 779, 782 (C.D. Cal. 2023) (discussing CIPA's "well-established 'party exception'"); 18 U.S.C. § 2511(2)(d) (setting forth Wiretap Act's party exception); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 145, 152 (3d Cir. 2015) (affirming dismissal of Wiretap Act and CIPA § 631(a) claims because defendant was a party to communications at issue). And "California courts interpret 'eavesdrop,' as used in [CIPA] § 632, to refer to a third party secretly listening to a conversation between two other parties." *Thomasson v. GC Servs. Ltd. P'ship*, 321 F. App'x 557, 559 (9th Cir. 2008). For this reason, the Ninth Circuit has held a plaintiff cannot prevail on a CIPA § 632 claim where the defendant was a party to the communication at issue. *Id.*; *see also, e.g.*, *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1089 (N.D. Cal. 2018). As a result, Meta is exempt from any wiretapping or eavesdropping liability under the federal and state statutes as a party to the communications at issue. *See, e.g.*, *Doe I*, 2024 WL 3490744, at *5; *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975). Courts routinely dismiss or grant summary judgment on wiretapping claims for this reason alone. For example, the Sixth Circuit affirmed summary judgment in a wiretapping case because the defendant was "a 'party to the communication.'" *Clemons v. Waller*, 82 F. App'x 436, 442 (6th Cir. 2003). The Ninth Circuit did the same in a CIPA § 632 case because a defendant's monitoring of its own phone call "cannot constitute eavesdropping." *Thomasson*, 321 F. App'x at 559; *see also, e.g.*, *B.K. v. Eisenhower Med. Ctr.*, 721 F. Supp. 3d 1056, 1065 (C.D. Cal. 2024) (dismissing Wiretap Act and CIPA § 631 claims with prejudice where defendant was a party to the underlying communications); *Pena v. GameStop, Inc.*, 670 F. Supp. 3d 1112, 1118–20 (S.D. Cal. 2023) (same); *Gonzales*, 305 F. Supp. 3d at 1089 (same for CIPA § 632 claim).

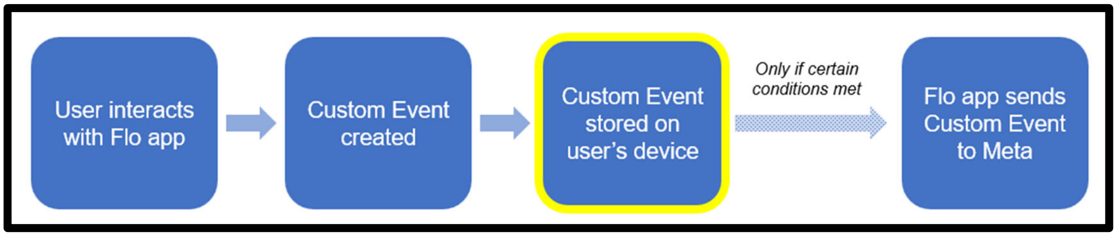
Even if plaintiffs were parties to Flo's communication of Custom Events to Meta (which the evidence does not support), the same result would hold because Meta was also a party to those communications. *See, e.g.*, *Clemons*, 82 F. App'x at 442; *Eisenhower Med. Ctr.*, 721 F. Supp. 3d at 1065; *Pena*, 670 F. Supp. 3d at 1118–20. Plaintiffs may rely on *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020), to argue the party exception should not apply here, but that case supports *Meta's* argument. In *Tracking Litigation*, the plaintiffs alleged Meta used certain "plug-ins," or programs, "to track users' browsing histories when they visit third-party websites." *Id.* at 596. When internet users visit a third-party website, their browsers send certain messages to the website's server. *Id.* at 607. The plaintiffs in *Tracking Litigation* alleged Meta's plug-ins directed browsers to "simultaneous[ly]" send "separate but identical" messages to Meta as well. *Id.* at 596, 607. The Ninth Circuit rejected Meta's party-exception argument, holding that "simultaneous, unknown duplication and communication of [the messages] do not exempt a defendant from liability under the party exception." *Id.* at 608. But here, there is no dispute that the Custom Events were neither simultaneous with nor a duplication of the information plaintiffs entered into the Flo app. *See supra* at pp. 5–6. Indeed, the Custom Event data were not a duplication (identical or otherwise) of anything transmitted to Flo, because the titles and parameters were *created* by Flo. App. 542–43, 722–23. Even plaintiffs' expert's analysis showed "the data that Flo and [Meta] may receive differ[]" and "were not duplicative." App. 720–23. And there is no dispute that the Custom Events were sent to Meta *after* they were stored, and not "simultaneous" with when plaintiffs entered information into the app. *See supra* at pp. 5–6; *infra* at pp. 12–13.

Because the undisputed evidence proves Meta did not "intercept" or "eavesdrop" on anything, the Court should enter judgment for Meta on plaintiffs' Wiretap Act and CIPA claims.

B. There Was No "Interception" While The At-Issue Communications Were "In Transit."

Meta cannot be held liable under the Wiretap Act or CIPA § 631(a) for another reason: any "interception" could not have happened "while [the communication] [was] in transit." Cal. Penal Code § 631(a); *see also Konop*, 302 F.3d at 878. The "in transit" requirement means any "interception" "must occur contemporaneous[ly] with the sending or receipt of the message." *Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 759 (N.D. Cal. 2023); *see also Konop*, 302 F.3d at 878 ("interception" under Wiretap Act requires "acquisition contemporaneous with transmission"). The Ninth Circuit has held "interception" of data "while it is [already] in electronic storage" does not qualify. *Konop*, 302 F.3d at 878–79. This includes any "temporary, intermediate" storage. *Id.* at 878 n.6. The fact that the "window during which an interception may occur is exceedingly narrow" is irrelevant: the interception must still occur "during transmission" to qualify as an "interception" under the statutes. *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1031 (N.D. Cal. 2014).

Here, there is no genuine factual dispute that the Custom Events were first stored on each Flo app user's device *before* any subsequent transmission to Meta, as illustrated below:


User interacts with Flo app
Custom Event created
Custom Event stored on user's device
Only if certain conditions met
Flo app sends Custom Event to Meta

App. 507–08, 718–20. Only *after* storage would the app send the Custom Events to Meta once certain conditions were met, such as having a reliable internet connection or reactivating the app after it was dormant on a user's device. App. 507–09. If, for example, a Flo app user was using the app on a flight, the Custom Events may not have been sent to Meta for hours. App. 509–10. And if a Flo app user turned off cellphone data for the Flo app or traveled internationally without a data plan, the Custom Events may not have been sent for days, weeks, or even longer. *Id.* Plaintiffs' own technical expert's analysis confirms Custom Events were first stored on users' devices before being transmitted to Meta. App. 718–20.

Applying the Ninth Circuit's decision in *Konop*, courts in this Circuit routinely grant dispositive motions when the challenged communications were not "intercepted" during transmission. *See, e.g.*, *Backhaut v. Apple Inc.*, 148 F. Supp. 3d 844 (N.D. Cal. 2015), *aff'd*, 723 F. App'x 405 (9th Cir. 2018) (granting summary judgment on Wiretap Act claim); *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (same); *Griffith v. TikTok, Inc.*, 2024 WL 5279224, at *10 (C.D. Cal. Dec. 24, 2024) (same for Wiretap Act and CIPA § 631(a) claims); *Sunbelt Rentals*, 43 F. Supp. 3d at 1033 (dismissing CIPA claim). In *Backhaut*, for example, the plaintiffs argued Apple's iMessage server caused non-Apple device users' messages "'to be intercepted at the exact moment of transmission as a result of a structural defect,' resulting in messages being sent as iMessages to users who cannot receive iMessages." 148 F. Supp. 3d at 850. Judge Koh entered summary judgment for Apple on the plaintiffs' Wiretap Act claim, holding "the undisputed evidence shows that any acquisition by [Apple] did not occur at the time of transmission as required by the Wiretap Act." *Id.* at 849. As Judge Koh explained, "[t]here can be no interception for purposes of the Wiretap Act if the acquisition of the message occurs while the message is in storage, even if it is in temporary storage incidental to the transmission of the communication." *Id.* at 849–50 (citing *Konop*). Similarly, in *Bunnell*, the court entered judgment for the defendant on the plaintiff's Wiretap Act claim because the email messages at issue were copied and forwarded only after being stored. 567 F. Supp. 2d at 1153–54. As that court explained, "the Ninth Circuit has determined . . . that the amount of time a message is in storage is immaterial," and transmission even "milliseconds" after the original communication occurred "does not constitute an 'interception.'" *Id.* at 1154 (citing *Konop*).

The Custom Events were stored *before* the Flo app transmitted them to Meta. The Court should therefore grant summary judgment to Meta on plaintiffs' Wiretap Act and CIPA § 631(a) claims.

C. Plaintiffs Cannot Prove That Meta Intended To "Intercept" Or "Eavesdrop."

There is another reason to grant summary judgment on plaintiffs' Wiretap Act and CIPA claims: plaintiffs must prove not just that Meta "intercepted" or "eavesdropped" on their communications, but that Meta *intended* to do so. CIPA § 632(a) requires proof that Meta "intentionally" "eavesdropped" on a "confidential communication." Cal. Penal Code § 632(a). Both the Wiretap Act and CIPA § 631(a) require proof that any "interception" was "intentional"—that is, that "the defendant acted consciously and deliberately with the goal of intercepting" the communications at issue. *United States v. Christensen*, 828 F.3d 763, 791 (9th Cir. 2015); *see also* 18 U.S.C. § 2511(1)(a); Cal. Penal Code

§ 631(a). Plaintiffs' theory is that Meta intended to "intercept" health information. *See* Dkt. 64 ¶¶ 400, 405, 411, 413; Dkt. 477 at 1. The record proves the opposite is true.

Throughout the class period, Meta indisputably and expressly prohibited Flo (and other app developers using Meta's SDK) from sending it any "health" information or other types of "sensitive personal data," as well as any data without "all necessary rights and permissions." *Supra* at p. 6. Flo also indisputably agreed to abide by that policy. *See id.* There is no evidence the policy was a pretense. To the contrary, when Meta first learned from the 2019 *WSJ* article that Flo was allegedly sending it health information, it built out its systems to detect and filter out "potentially health-related data." App. 272–73, 275. There is no evidence that, despite these efforts, Meta secretly *wanted* to receive health information—let alone evidence showing this is a "genuine issue for trial." *Celotex*, 477 U.S. at 324. Instead, granting every inference in plaintiffs' favor, the record at most shows that ***if*** Meta received any health information from Flo, that was because Flo unilaterally decided to send it in violation of Meta's terms. *See supra* at pp. 4–6. Holding Meta liable for receiving that information would be like holding someone liable for receiving a package containing something he expressly told the sender never to send.

Courts have declined to hold a party liable under the wiretapping statutes for receiving unwanted health information. In *Doe I v. Google*, for example, the plaintiffs brought Wiretap Act and CIPA claims alleging that healthcare providers transmitted personal health information to Google using Google's source code. 2024 WL 3490744, at *1. Judge Chhabria dismissed those claims, holding that "the plaintiffs ha[d] not adequately alleged that Google intentionally obtained patients' private health information." *Id.* at *4. He explained that Google had "repeatedly told developers not to send personally identifiable information through use of its source code," with the "takeaway" being that "Google purposefully acted so as *not* to receive any personal health information." *Id.* Similarly, in *B.K. v. Desert Care Network*, 2024 WL 1343305 (C.D. Cal. Feb. 1, 2024), the court dismissed a CIPA claim based on allegations that the defendants had installed certain code created by Meta on their hospital websites and that this code allowed Meta to intercept information about medical appointments, prescriptions, and test results entered onto those websites. *Id.* at *1. The plaintiffs' complaint "repeatedly mention[ed] Meta's express desire not to receive health data from its business partners," as demonstrated by Meta's Business Tools Terms. *Id.* at *7. The "Plaintiffs' allegations indicate that Meta either had no intention of receiving the data at issue or had some alternative mens rea not rising to the level of intentionality." *Id.* The same is true here: there is no genuine dispute that Meta not only expressly prohibited Flo and other developers from sending it health and other sensitive information, but also took steps to enforce that policy. *See supra* at pp. 6, 14; *see also, e.g.*, *Sunbelt Rentals*, 43 F. Supp. 3d at 1030 (dismissing wiretapping claims because counter-defendant "did not intentionally capture or redirect" the messages at issue). And there is no evidence showing Meta secretly harbored some contrary intent.

Courts regularly grant summary judgment if the plaintiffs do not present evidence of intent. *See, e.g.*, *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742–43 (4th Cir. 1994); *Forsyth v. Barr*, 19 F.3d 1527, 1535–36 (5th Cir. 1994); *Cantu v. Guerra*, 2023 WL 5217852, at *23 (W.D. Tex. Aug. 11, 2023). For example, in *Global Imaging Acquisitions Group, LLC v. Rubenstein*, 2017 WL 11673437 (E.D. Wis. Aug. 16, 2017), the court granted summary judgment to a defendant on a Wiretap Act claim, explaining that the defendant had received the messages at issue only because *another* defendant "had programmed his Apple iCloud account to send copies of all communications sent through that account to [the defendant]." *Id.* at *11. The court reasoned it was "unlikely" Congress would have intended to make the innocent receipt of unwanted information "a federal crime," noting the absence of cases supporting that result. *Id.* The same logic applies here: Meta never wanted health information, took affirmative steps to *avoid* receiving it, and should not be held liable if Flo decided to send it anyway.

The Court's rejection of Google's argument that it did not "'purposefully' or 'intentionally' intercept[] Flo App Data without user consent" (Dkt. 338 at 24; Dkt. 485 at 7) does not foreclose an intent argument from Meta. The cases cited above rejecting the notion that a party can be held liable for wiretapping or eavesdropping based on the receipt of unwanted information were not before the Court when it addressed Google's argument, and Google's argument in its motion regarding the requisite intent for plaintiffs' wiretapping claims did not point to language in its contracts with developers like the language in Meta's Business Tools Terms that prohibit the sending of "health" or other "sensitive" information via Meta's SDK. *See* Dkt. 338 at 23–25.

The Court should enter judgment for Meta on plaintiffs' Wiretap Act and CIPA claims because, accepting every inference in plaintiffs' favor, it never intended to "intercept" or "eavesdrop" on anything. *See, e.g.*, *Sanders*, 38 F.3d at 742–43; *Forsyth*, 19 F.3d at 1535–36; *Cantu*, 2023 WL 5217852, at *23; *Glob. Imaging*, 2017 WL 11673437, at *11.

D. Plaintiffs' Wiretap Act And CIPA Claims Are Barred By Consent.

Plaintiffs cannot prevail on their Wiretap Act and CIPA claims for still another cross-cutting reason: they and Flo alike consented to the sharing of Custom Events with Meta. Lack of consent is an essential element of plaintiffs' CIPA claims, Cal. Penal Code §§ 631(a), 632, and consent is also an affirmative defense to plaintiffs' Wiretap Act claim, 18 U.S.C. § 2511(2)(d). The undisputed evidence proves that plaintiffs consented here, and Flo's consent alone bars plaintiffs' Wiretap Act claim.

1. Plaintiffs Consented To The Data Sharing At Issue, Barring Their Wiretap Act And CIPA Claims.

Even taking as true plaintiffs' theory that Meta "intercepted" communications between plaintiffs and Flo, Meta would *still* be exempt from liability under the Wiretap Act because plaintiffs consented to any "interception" by Meta. The undisputed evidence shows that all but one of the plaintiffs (Ms. Chen)[2] used Facebook during the class period and thus agreed to Meta's terms and policies, including its Terms of Service and Data Policy. App. 222–23, 227, 255–56, 295, 323, 349, 377, 404, 879–81, *see also Lloyd v. Facebook, Inc.*, 2023 WL 1802415, at *1 (N.D. Cal. Feb. 7, 2023), *aff'd in part*, 2024 WL 3325389 (9th Cir. July 8, 2024) (Meta's "relationship with [its] users . . . is governed by its Terms of Service," "to which all users must agree to create a Facebook account"); *Meta Platforms, Inc. v. Nguyen*, 2023 WL 8686924, at *2 (N.D. Ca. Nov. 21, 2023) (similar). These terms and policies contain clear and broad disclosures informing users that Meta may receive data reflecting their activity on third-party apps that use Meta's Business Tools, including its SDK. *See, e.g.*, App.

[2] Ms. Chen cannot prevail on her claims because there is no evidence showing Meta could associate her with any information it received from Flo, let alone any purported health information. She did not have an Instagram or Facebook account during the proposed class period, so Meta would not have been able to specifically link any Custom Events to her account. App. 120–22, 243–44. Any Custom Events received by Meta and relating to Ms. Chen's use of the app would thus have been anonymous. Ms. Chen cannot assert privacy claims based on anonymized data. *See, e.g.*, *Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017); *Mikulsky v. Noom, Inc.*, 2024 WL 251171, at *5 (S.D. Cal. Jan. 22, 2024). Meta respectfully disagrees with the Court's ruling to the contrary in its order deciding Google's summary-judgment motion. Dkt. 485 at 3.

47, 57–58, 67. Meta's Data Policy explains at length that Meta "collect[s]" and "receive[s]" "information about the . . . apps [users] visit," "how [users] use [developers'] services," "as well as information the developer or publisher of the app" chooses to send to Meta. App. 33, 47; *see also, e.g.*, App. 39, 57–58, 67. These policies "expressly disclosed [Meta's] intention to track [users'] activity on third-party apps" that use Meta's SDK. *Hammerling v. Google LLC*, 2024 WL 937247, at *3 (9th Cir. Mar. 5, 2024).

In a case much like this one, the Ninth Circuit held that a Facebook user's consent to Meta's Data Policy was sufficient to qualify as consent to Meta's subsequent collection of that user's "health-related data." *Smith*, 745 F. App'x at 9. In *Smith*, the plaintiffs alleged that the defendants disclosed information about the plaintiffs' web-browsing activity to Meta by embedding in their website another one of Meta's Business Tools, known as the "pixel." 262 F. Supp. 3d 943, 948–49 (N.D. Cal. 2017). Meta's pixel works like the SDK, except the pixel is used for websites rather than apps. *See id.* The district court held the plaintiffs had "consented to Facebook's tracking activity" and pointed to Meta's Data Policy, which disclosed "the precise conduct at issue in th[at] case," i.e., that Meta "collect[s] information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button . . .)." *Id.* at 953–54. The district court also rejected the plaintiffs' arguments that the Data Policy was "too . . . 'broad' to be enforceable," explaining that "a contractual term is not ambiguous just because it is broad." *Id.* at 954. The Ninth Circuit affirmed: "A reasonable person viewing those disclosures would understand that Facebook maintains the practice of (a) collecting its users' data from third-party sites and (b) later using the data for advertising purposes," and "[k]nowing authorization of the practice constitutes [p]laintiffs' consent." *Smith*, 745 F. App'x at 8–9; *see also Lloyd*, 2024 WL 3325389, at *2 (similar).

This case presents substantively identical facts: seven of the eight plaintiffs consented to the same Meta Data Policy as the Facebook and Instagram users in *Smith*, and that policy disclosed the precise data sharing that they now challenge. Judgment should therefore be entered for Meta as to those plaintiffs' Wiretap Act and CIPA claims. Under the Wiretap Act, an "interception" is not unlawful "where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). Courts have also dismissed Wiretap Act claims because the plaintiffs consented to the conduct they challenge, including based on Meta's Data Policy. *See, e.g.*, *Smith*, 262 F. Supp. 3d at 955. Courts have similarly dismissed CIPA claims where the "plaintiffs consented to the collection of data at issue," including based on Meta's Data Policy. *Silver v. Stripe Inc.*, 2021 WL 3191752, at *4–5 (N.D. Cal. July 28, 2021); *see also, e.g.*, *Garcia v. Enter. Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135–37 (N.D. Cal. Jan. 23, 2015); *Smith*, 262 F. Supp. 3d at 955.

Although a few district courts have reached a contrary outcome at the pleadings stage, those decisions run counter to the Ninth Circuit's holding in *Smith*. *See In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 1002–03 (N.D. Cal. 2024); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793 (N.D. Cal. 2022). There, the courts reasoned that, where *sensitive* data is involved, "generalized notice" about data collection reflecting activity on third-party websites is not enough to support dismissal, and Meta's policies must "specifically indicate" Meta will receive the specific data at issue to establish consent. *Meta Pixel Healthcare*, 647 F. Supp. 3d at 793 (health information); *see also Meta Pixel Tax*, 724 F. Supp. 3d at 1003–04 (tax information). But *Smith* foreclosed that theory. The Ninth Circuit expressly rejected the plaintiffs' argument that they provided only "general consent" and "did not consent to the collection of health-related data due to its 'qualitatively different' and 'sensitive' nature." 745 F. App'x at 9. In affirming dismissal of claims about Meta's receipt of "browsing data from various healthcare-related websites," *id.* at 8, the court did not ask whether Meta's policies "specifically indicated" it would receive "healthcare-related" data. There is no basis for that extra requirement, which improperly cabins otherwise broad language and imposes judicially crafted carveouts on otherwise broad disclosures. Instead, the court noted "many other kinds of [web-browsing] information are equally sensitive" and held "the practice complained of falls within the scope of [p]laintiffs' consent to Facebook's Terms and Policies." *Id.* at 9. The same logic applies here.

Nor does the Court's rejection of Google's consent argument compel a similar outcome here. The Court concluded "Google hangs its hat for the defense of consent solely on plaintiffs' acceptance of Flo's privacy policies," which, as this Court noted, differed "over the years," thus raising disputes about "the scope of plaintiffs' consent." Dkt. 485 at 3–4. Meta's Data Policy, which the Court did not consider in connection with Google's motion for summary judgment, indisputably disclosed the challenged data sharing throughout the proposed class period. *See supra* at p. 6. The Court should follow the Ninth Circuit's reasoning in *Smith* and grant judgment for Meta on seven of the eight plaintiffs' Wiretap Act and CIPA claims.

2. Flo Consented To The Challenged "Interception," Barring The Wiretap Act Claim.

Meta is also exempt from liability under the Wiretap Act because Flo consented to the "interceptions" that plaintiffs theorize. The Wiretap Act is a one-party-consent statute, meaning it exempts from liability any "interception" "where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). Flo chose to integrate the SDK into its app. *See* App. 505, 655–56. And Flo created and named all its Custom Events and chose to send them to Meta. App. 506–07. It is thus undisputed that Flo consented to any alleged "interception" by Meta of the Custom Event data at issue.

Courts regularly dismiss Wiretap Act claims under such circumstances. *See, e.g.*, *Katz-Lacabe v. Oracle Am., Inc.*, 2024 WL 1471299, at *4 (N.D. Cal. Apr. 3, 2024). For example, in *Katz-Lacabe*, the plaintiffs alleged the defendant had collected their internet activity through different technological tools used by third-party websites. *Id.* at *1. The court dismissed the plaintiffs' Wiretap Act claim, holding that the websites "agreed to deploy [the defendant's] data collection tool" and thus consented to any resulting interception. *Id.* at *4. Flo's consent is even more evident here: Flo integrated Meta's SDK into its app code and created and named the Custom Events, and its app sent the data to Meta.

II. Plaintiffs Cannot Prove Essential Elements Of Their CDAFA Claim.

Meta is entitled to summary judgment on plaintiffs' CDAFA claim for four reasons: (1) there is no evidence Meta "actively participated" in "hacking"; (2) there is no evidence Meta "knowingly" participated in "hacking"; (3) consent bars their CDAFA claim; and (4) there is no evidence plaintiffs suffered the requisite "damage or loss" under the statute.

No evidence Meta "actively participated" in "hacking." The CDAFA is "an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose." *Sunbelt Rentals*, 43 F. Supp. 3d at 1032. Its provisions "generally prohibit[] tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." *CTI III, LLC v. Devine*, 2022 WL 1693508, at *3 (E.D. Cal. May 26, 2022) (cleaned up). A plaintiff must prove the defendant "actively participated" in such hacking to fall within the CDAFA's ambit. *Id.* at *4; *see also, e.g.*, *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011) ("the relatively few cases interpreting the [CDAFA] largely seek to impose liability against individuals or entities who are alleged to have actually participated in [the] unauthorized [behavior]").

Here, there is no evidence Meta "actively participated" in any "hacking." Meta simply made its SDK publicly available. App. 502–03. Developers could then choose whether to use it, subject to Meta's terms. *See supra* at pp. 4–6. Flo chose to integrate Meta's SDK into its app code, create the challenged Custom Events, and send that information to Meta. *See id.* Meta's passive role in this process did not amount to "active[]" "hacking." *See CTI III*, 2022 WL 1693508, at *4; *Claridge*, 785 F. Supp. 2d at 863. Meta is thus entitled to summary judgment on plaintiffs' CDAFA claim. *See Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020) (dismissing CDAFA claim where defendant "was [not] involved in the hacking itself, directly or indirectly"); *cf. Welenco, Inc. v. Corbell*, 126 F. Supp. 3d 1154, 1170 (E.D. Cal. 2015) (granting defendant summary judgment on CDAFA claim where challenged conduct did not "resemble[]" "'hacking[]' behavior").

No evidence Meta "knowingly" participated in "hacking." Plaintiffs' CDAFA claim also runs into the same insurmountable obstacle as its Wiretap Act and CIPA claims. Plaintiffs must prove Meta "[k]nowingly" violated the CDAFA "without permission." Cal. Penal Code § 502(b)(12), (c)(1)–(3), (6)–(8), (13). Thus, plaintiffs must prove Meta knowingly and actively "hacked" Flo app users' devices and data without their permission. *See supra* at pp. 19–20; *CTI III, LLC*, 2022 WL 1693508, at *4; *Claridge*, 785 F. Supp. 2d at 863; *Sunbelt Rentals*, 43 F. Supp. 3d at 1032. The record does not support that theory of liability. Just as there is no evidence that Meta actively participated in any "hacking" in the first place, there is also no evidence Meta *knowingly* and actively "hacked" any device or data. To the contrary, beyond requiring that Flo not send Meta any "health" or other "sensitive" information, send only data it had "all necessary rights and permissions" to send, and disclose use of Meta's SDK to Flo app users, *see supra* at p. 6, there is no evidence that Meta had any awareness of what Flo ultimately told its users with respect to data collection. Meta is entitled to summary judgment on plaintiffs' CDAFA claim for this reason. *See Nowak*, 2020 WL 6822888, at *5 (dismissing CDAFA claim given plaintiff's failure to allege defendant "had the requisite knowledge to impose liability for assisting the hacking").

Consent bars plaintiffs' CDAFA claim. Plaintiffs' consent to Meta's terms and policies, *see supra* at pp. 6, 16–19, means that plaintiffs cannot satisfy CDAFA's requirement that a statutory violation was committed "without permission." Cal. Penal Code § 502(c). Courts have dismissed CDAFA claims where a defendant has authorization to access the plaintiffs' data. *See, e.g.*, *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 131–32 (N.D. Cal. 2020). For example, in *Brodsky*, the plaintiffs asserted a CDAFA claim, alleging Apple "knowingly and without permission accessed, altered, or otherwise disrupted Plaintiffs' Apple devices" by requiring use of a two-factor login authentication tool without their consent. *Id.* at 116–17, 131 (cleaned up). While the plaintiffs challenged Apple's access to their "login activities," such as their usernames and passwords, through the two-factor login authentication tool, they did not challenge Apple's access to those "activities" through other login methods. *Id.* at 119, 132. The court dismissed the CDAFA claim, reasoning the plaintiffs were "only challeng[ing] the login method of [two-factor authentication] without alleging that Apple is otherwise accessing Plaintiffs' login activities [through other means]." *Id.* at 132. Here, the record shows Meta received the Custom Events with plaintiffs' authorization, since they agreed to Meta's Data Policy. *See supra* at pp. 6, 16–19. Plaintiffs cannot prevail on their CDAFA claim as a result. *See Brodsky*, 445 F. Supp. 3d at 131–32; *cf. Welenco*, 126 F. Supp. 3d at 1170.

No evidence of requisite "damage or loss." The CDAFA provides that only someone who has "suffer[ed] damage or loss by reason of a violation" of the statute may bring a civil action "for compensatory damages and injunctive relief or other equitable relief." Cal. Penal Code § 502(e)(1). And it permits recovery of "[c]ompensatory damages [that] include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id.* Thus, to prevail on their CDAFA claim, plaintiffs must prove they suffered "damage or loss" as a result of Meta's active "hacking" of plaintiffs' devices. But even if the Court assumed for the sake of argument that Meta actively and knowingly "hacked" plaintiffs' devices without permission, plaintiffs still could not prevail because they cannot show any resulting damage or loss.

This Court denied Google's motion for summary judgment on plaintiffs' CDAFA claim, rejecting Google's argument that an "intangible invasion of privacy" is not "damage or loss" under the statute. Dkt. 485, at 4–5. The Court reasoned that "[t]he plain language of the CDAFA is not as definitive as Google urges." *Id.* at 5 (citing Cal. Penal Code § 502(a)). And the Court concluded that, even under Google's interpretation of the statute, there was "evidence from which a reasonable jury could conclude that the information obtained by Google 'carried financial value' that amounts to damage or loss suffered by plaintiffs." *Id.* This Court's ruling is one of only a few cases reaching this result—and runs counter to a broad consensus of decisions that were not cited in the briefing on Google's motion. Meta encourages the Court to reconsider its reasoning in light of those cases.

The overwhelming majority of courts have held that "alleged privacy invasions do not qualify under the statute." *Heiting*, 709 F. Supp. 3d at 1020. Privacy invasions that do not qualify include the loss of the right to control data, the loss of the value of data, and the loss of the right to protect data. *See, e.g.*, *id.*; *Ingrao v. AddShoppers, Inc.*, 2024 WL 4892514, at *15–16 (E.D. Pa. Nov. 25, 2024); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1081–83 (N.D. Cal. 2023); *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d at 148–149, 152; *In re Google Android Consumer Priv. Litig.*, 2013 WL 1283236, at *11 (N.D. Cal. Mar. 26, 2013). Likewise, unlawful *access* to communications, notes, and medical information does not qualify as "damage or loss" under the CDAFA. *See Pratt v. Higgins*, 2023 WL 4564551, at *9 (N.D. Cal. July 17, 2023). As all these courts have recognized, such "damage or loss" must include "some damage to the computer system, network, program, or data contained on that computer, as opposed to data generated by a plaintiff while engaging with a defendant's website." *Heiting*, 709 F. Supp. 3d at 1021; *see also, e.g.*, *Ingrao*, 2024 WL 4892514, at *16; Cal. Penal Code § 502(e)(1). Plaintiffs have no evidence to that effect and, instead, point to their own privacy interests as the source of their purported injury. *See* App. 212, 217, 224, 232, 237, 242, 249, 254.

This Court, in deciding Google's motion for summary judgment, relied on two anomalous cases in holding that the loss in value of misappropriated data is sufficient to show damage or loss under the CDAFA. *See Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934, 945 (S.D. Cal. 2024); *Brown v. Google, LLC*, 685 F. Supp. 3d 909, 940 (N.D. Cal. 2023). Those cases were wrongly decided because they improperly expanded the scope of injury covered by the CDAFA by misconstruing the Ninth Circuit's decision in *Tracking Litigation*. *Brown*, 685 F. Supp. 3d at 940 (citing *Tracking Litigation*); *Esparza*, 723 F. Supp. 3d at 945 (citing *Brown*); *compare Heiting*, 709 F. Supp. 3d at 1021 (disagreeing with reasoning in *Brown*). *Tracking Litigation* does not support *Brown*'s holding, *Esparza*'s holding, or plaintiffs' CDAFA claims. 956 F.3d at 599–601. For one thing, as Judge Chhabria has explained, *Tracking Litigation* decided "only that the plaintiffs had an entitlement to the profits earned off personal data for purposes of *Article III standing*," not the CDAFA. *Doe I*, 2024 WL 3490744, at *7 (emphasis added). For another, even under Article III, *Tracking Litigation* requires plaintiffs to show damages and to plead "they retain a stake in the profits garnered from their personal [information] because the circumstances are such that, as between the two parties, it is *unjust* for Facebook to retain it." 956 F.3d at 600 (cleaned up). Thus, even if plaintiffs' data "carried financial value" (Dkt. 485 at 5), that would be insufficient to show Article III harm based on *Tracking Litigation*'s reasoning. There is no evidence that plaintiffs "retain a stake in the profits" from their data or that Meta was unjustly enriched by collecting their data. *Tracking Litigation*, 956 F.3d at 600. And as discussed above, there is no evidence that plaintiffs suffered any damage or loss sufficient under the CDAFA. *See supra* at pp. 21–23; *Roe v. Amgen Inc.*, 2024 WL 2873482, at *6–7 (C.D. Cal. June 5, 2024) (no damage or loss under CDAFA where plaintiffs did not allege defendants sold their data or offer facts indicating unjust enrichment). Without more, plaintiffs cannot prevail on their CDAFA claim. In line with the overwhelming majority of caselaw, this Court should grant summary judgment for Meta on plaintiffs' CDAFA claim.

III. Plaintiffs Cannot Prove Essential Elements Of Their "Aiding And Abetting" Intrusion-Upon-Seclusion Claim.

Meta is entitled to summary judgment on plaintiffs' "aiding and abetting" claim because (1) there is no evidence showing Meta had the requisite mens rea; and (2) the claim is barred by consent.

No evidence Meta "knew" about and "substantially assisted" tortious activity. Plaintiffs' "aiding and abetting" intrusion-upon-seclusion claim requires proof Meta knew about Flo's allegedly deceptive disclosure practices. *See* Dkt. 485 at 5–6. More specifically, an "aiding and abetting" claim requires proof Meta "kn[ew] [Flo's] conduct constitutes a breach of duty," *Fiol v. Doellstedt*, 50 Cal.

App. 4th 1318, 1325 (1996), and "reach[ed] a conscious decision to participate in tortious activity for the purpose of assisting [Flo] in performing a wrongful act," *Howard v. Superior Ct.*, 2 Cal. App. 4th 745, 749 (1992). There is no evidence showing Meta had such knowledge or decided to "assist[]" Flo in any wrongful act. Google sought summary judgment on plaintiffs' "aiding and abetting" claim on this basis, arguing it did not know about any underlying privacy violation and did not substantially assist Flo in violating plaintiffs' privacy. *See* Dkt. 338 at 22–23. The Court ruled in Google's favor, finding the record "devoid" of any facts showing Google had "actual knowledge of Flo's deceptive disclosure practices with respect to plaintiffs' private health information." Dkt. 485 at 5.

The same is true for Meta: granting every inference in plaintiffs' favor, there is not a shred of evidence that Meta was aware Flo made any purportedly false representations, let alone that Meta substantially assisted or encouraged them. To the contrary, Meta required Flo to send only data it had "all necessary rights and permissions" to send, and to not send any "health" or other "sensitive" information. *Supra* at p. 6. Because there is no evidence Meta knew of any purportedly tortious conduct, there necessarily is no evidence that Meta "reach[ed] a conscious decision to participate in [that] activity *for the purpose of* assisting [Flo]" in that conduct. *Howard*, 2 Cal. App. 4th at 749 (emphasis added). As this Court explained in connection with Google's motion for summary judgment, any "after-the-fact events" cannot suffice, such as any "suggestion that [Meta] could have used data obtained by Flo," because those events "do not establish that [Meta] knew it was assisting Flo in committing a tort." Dkt. 485 at 5–6. The Court should grant summary judgment for Meta on this claim as well. *Id.*; *Trabulsi v. Wells Fargo Bank, Nat'l Ass'n*, 2018 WL 6444897, at *3 (C.D. Cal. Nov. 16, 2018); *Chance World Trading E.C. v. Heritage Bank of Com.*, 438 F. Supp. 2d 1081, 1084 (N.D. Cal. 2005), *aff'd*, 263 F. App'x 630 (9th Cir. 2008).

Consent bars plaintiffs' "aiding and abetting" claim. To prevail on their "aiding and abetting" claim, plaintiffs must prove the underlying tort, i.e., that Flo intruded upon plaintiffs' privacy. *Yazdanpanah v. Sacramento Valley Mortg. Grp.*, 2009 WL 4573381, at *5 (N.D. Cal. Dec. 1, 2009). But courts have dismissed claims for intrusion upon seclusion based on the plaintiffs' consent, including consent based on the same Meta Data Policy at issue here. For example, in *Smith*, the Ninth Circuit affirmed the district court's dismissal of the plaintiffs' intrusion-upon-seclusion claim because the plaintiffs had consented to the challenged data-sharing practices based on their acceptance of Meta's Data Policy. 745 F. App'x at 8. The same logic applies with equal force to plaintiffs' "aiding and abetting" claim: the Data Policy discloses the very conduct that plaintiffs now seek to challenge. *See supra* at pp. 6, 16–19. This, too, supports granting summary judgment in favor of Meta on this claim.

IV. Plaintiffs Cannot Prove Essential Elements Of Their UCL Claims.

Although plaintiffs represented that their UCL claims are "moot" (Dkt. 348 at 17 n.18), and the Court entered judgment on those claims for Google on that basis, finding plaintiffs had "abandoned" them (Dkt. 485 at 4), plaintiffs have refused to withdraw them (App. 2). In any event, plaintiffs cannot prevail on those claims for at least three reasons. First, plaintiffs cannot satisfy the UCL's requirement that they "lost money or property." *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011). It is "widely" recognized that harm involving the loss of "personal information" is not an economic injury, and plaintiffs have not pointed to any other purportedly economic harm. *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at *8 (N.D. Cal. Mar. 5, 2021); *supra* at p. 22; *see also, e.g.*, *In re Facebook Priv. Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011), *aff'd*, 572 F. App'x 494 (9th Cir. 2014). Second*,* plaintiffs' "aiding and abetting" UCL claim is based on the same conduct as their "aiding and abetting" intrusion-upon-seclusion claim (Flo's purportedly deceptive disclosures) (*see* Dkt. 64 ¶¶ 377–91), but there is no evidence Meta "knew" about and "substantially assisted" Flo's alleged conduct. *See supra* at pp. 23–24. Third, plaintiffs' consent bars their UCL claims. *See Vasquez v. Leprino Foods Co.*, 2021 WL 1737480, at *6 (E.D. Cal. May 3, 2021); *supra* at pp. 6, 16–19.

CONCLUSION

The Court should grant Meta's motion because there is no genuine dispute of material fact as to any of the claims against Meta. The Court should do so regardless of how it resolves plaintiffs' pending motion for class certification, because the issues discussed above are dispositive not only of the named plaintiffs' claims, but also the claims of the entire proposed class.

Dated: February 6, 2025

/s/ *Elizabeth K. McCloskey*
GIBSON, DUNN & CRUTCHER LLP
Christopher Chorba (SBN 216692)
333 South Grand Avenue
Los Angeles, CA 90071
Telephone: 213.229.7503
CChorba@gibsondunn.com

Elizabeth K. McCloskey (SBN 268184)
Abigail A. Barrera (SBN 301746)
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200
EMcCloskey@gibsondunn.com
ABarrera@gibsondunn.com

LATHAM & WATKINS LLP
Melanie M. Blunschi (Bar No. 234264)
melanie.blunschi@lw.com
Kristin Sheffield-Whitehead (Bar No. 304635)
kristin.whitehead@lw.com
Catherine A. Rizzoni (Bar No. 322267)
cat.rizzoni@lw.com
505 Montgomery St., Suite 2000
San Francisco, CA 94111
Telephone: +1.415.391.0600

Andrew B. Clubok (*pro hac vice*)
andrew.clubok@lw.com
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Telephone: +1.202.637.2200

Michele D. Johnson (Bar No. 198298)
michele.johnson@lw.com
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626
Telephone: +1.714.540.1235

Counsel for Defendant Meta Platforms, Inc.
(formerly known as Facebook, Inc.)